IN THE CLAIMS

Claims 1-11   (Canceled)

12.   (New) A method for fast generation of a cryptographic key, comprising:
generating a first public key for encrypting a first wireless communication; and
generating, upon termination of the first wireless communication, a second public key for use in a second wireless communication,
wherein the second public key is independent of the first public key.

13.   (New) The method of claim 12, further comprising:
determining whether the second public key has been stored.

14.   (New) The method of claim 13, further comprising:
using the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

15.   (New) The method of claim 13, further comprising:
generating a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

16.   (New)   A wireless communication device for fast generation of a cryptographic key, comprising:
means for generating a first public key for encrypting a first wireless communication; and
means for generating, upon termination of the first wireless communication, a second public key for use in a second wireless communication,
wherein the second public key is independent of the first public key.

2

17.   (New)   The wireless communication device of claim 16, further comprising:

means for determining whether the second public key has been stored.

18.   (New)   The wireless communication device of claim 17, further comprising:

means for using the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

19.   (New)   The wireless communication device of claim 17, further comprising:

means for generating a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

20.   (New)   A wireless communication device for fast generation of a cryptographic key, comprising:

a processor for generating a first public key to encrypt a first wireless communication and generating, upon termination of the first wireless communication, a second public key for use in a second wireless communication; and

a memory for storing the second public key,

wherein the second public key is independent of the first public key.

3